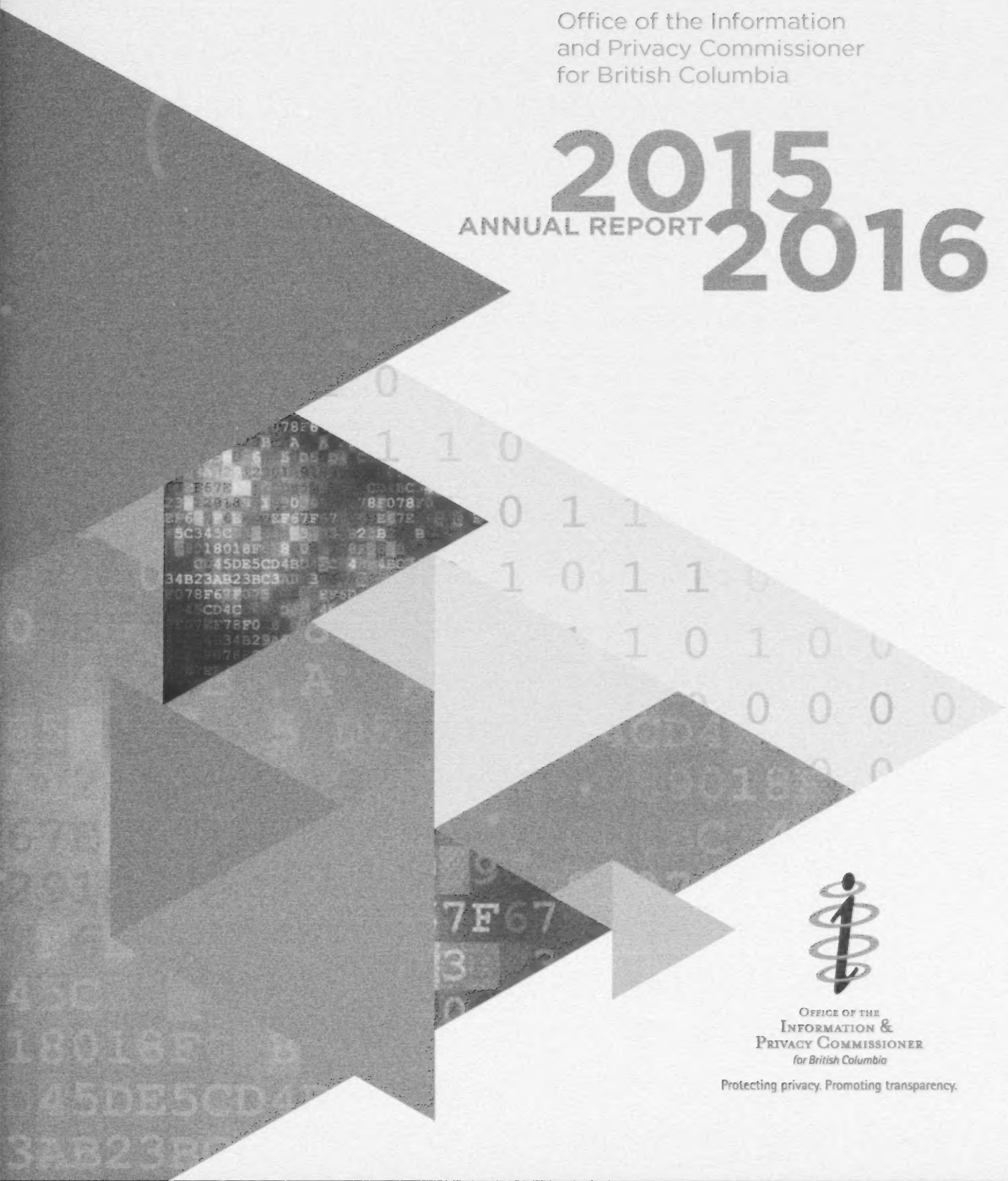
Office of the Information and Privacy Commissioner for British Columbia

2015/2016 ANNUAL REPORT



OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

Protecting privacy. Promoting transparency.

Who we are

Established in 1993, the Office of the Information and Privacy Commissioner provides independent oversight and enforcement of B.C.'s access and privacy laws, including:

- The ***Freedom of Information and Protection of Privacy Act*** ("FIPPA"), which applies to over 2,900 "public bodies," including ministries, local governments, schools, crown corporations, hospitals, municipal police forces and more;
- The ***Personal Information Protection Act*** ("PIPA"), which applies to over 380,000 private sector "organizations," including businesses, charities, associations, trade unions and trusts.

Elizabeth Denham is B.C.'s current Information and Privacy Commissioner.

Our Vision

- A community where privacy is valued, respected and upheld in the public and private sectors;
- A community where access to information rights are understood and robustly exercised;
- A community where public agencies are open and accessible to the citizenry they serve.

Strategic Goals (2015-2016)

1. Uphold privacy rights and monitor protection of personal information and data.
2. Ensure public bodies and private sector organizations understand their responsibilities under the law.
3. Promote and advocate for an open, accountable and transparent public sector.
4. Help individuals understand the value of information rights and to make informed choices about the exercise of those rights.
5. Enhance the quality and capacity of the OIPC's people, systems, processes and culture.

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

July 2016

The Honourable Linda Reid
Speaker of the Legislative Assembly
of British Columbia
Room 207, Parliament Buildings
Victoria, BC V8V 1X4

Honourable Speaker:

In accordance with s. 51 of the *Freedom of Information and Protection of Privacy Act*, I have the honour of presenting the Office's Annual Report to the Legislative Assembly.

This report covers the period from April 1, 2015 to March 31, 2016.

Yours sincerely,

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

Table of Contents

Commissioner's Message	4
Our Work	6
Highlights 2015-16	8
Compliance Summary	12
FIPPA Reviewed	14
Access Denied	16
In the Public Interest	18
Final Outcome	20
Surveillance Society	22
Year in Numbers	24
Financial Reporting	33
Resources	35

COMMISSIONER'S MESSAGE

"This is the sixth annual report I have had the honour to present to the Legislative Assembly for the Office of the Information and Privacy Commissioner. It is also my last annual report for this Office, as my six-year term ends July 6, 2016."

— Elizabeth Denham,
Information and Privacy Commissioner for British Columbia

When I came to this Office in 2010, I set out many goals for myself and my staff. I wanted to build a proactive office with a policy and technology focus. I wanted to advocate for more privacy management programs that anticipate rather than just react to privacy breaches. And I wanted to assemble an audit program.

Through dedication and hard work my staff and I have achieved these goals and our work has made a positive difference to the citizens of British Columbia. We have raised the profile of the Office, not just in British Columbia, but around the world. I am very proud that the OIPC will take the lead this summer as Secretariat for the Asia Pacific Privacy Authorities, an international forum for privacy regulators to create partnerships and exchange ideas.

As I write this message, I reflect on the volume of work my Office has completed in the past six years: 295 Orders and Decisions, 36 Investigations and Special Reports and three Audits.

All of this work is important. But some of it stands above the rest.

Our broad investigation into police information checks in 2014 resulted in a province-wide policy change that saw the elimination of mental health information from all record checks. Non-conviction information also ceased to be disclosed for all jobs outside the vulnerable sector.

This Office also pulled back the curtain on new technologies, from automatic licence plate recognition systems to facial recognition to employee monitoring and spyware. As a regulator, I believe that we have a crucial role to play in this area. We help the public understand new technologies and their impact on privacy and we educate businesses and public bodies so they understand their limits.

As this annual report indicates, 2015-16 has been the busiest year in my term. When I released my first annual report in 2009-10, we reported receiving 5,970 files for the fiscal year. Today that number has jumped to 9,024 files, an increase of 51%. My staff is working diligently to handle this volume and has successfully implemented a Continuous Improvement Process. We are now closing files faster while still maintaining administrative fairness and a high level of public service.

Access Denied, the deleted email investigation I released in October 2015, prompted a commitment from government to pass duty to document legislation and other key access to information policy changes. This will ensure better public record keeping, greater accountability for citizens and more robust information rights, because records will be created and retained.

In another notable 2015 file, our legal analysis and findings revealed that key features of the District of Saanich's employee monitoring software violated the privacy rights of its staff and elected officials. My Office reminded the District that employees have a reasonable expectation of privacy at work, even when using a computer or mobile device supplied by an employer.

We closely examined health authorities in 2015 in this Office's second examination in our Audit and Compliance program. In this proactive report, I called for immediate action to address the gaps we found in the privacy breach management practices of B.C.'s health authorities and recommended strong policies, compliance monitoring and training of health care providers and staff.

My Office's participation in the mandated review of the *Freedom of Information and Protection of Privacy Act* by a Special Committee, which began in the summer of 2015, led to some important results in 2016. Not surprisingly, the findings in the *Access Denied* report prompted many of my recommendations to the Committee. If government accepts the Committee's recommendations, British Columbia will lead Canada as the first jurisdiction to bring a statutory duty to document into force.

Finally, I want to mention the work we have done to bring diverse groups together. In April 2016, my Office partnered with the Conference Board of Canada to host a Canadian Privacy Summit in Vancouver. Chief Privacy Officers and major players in government and civil society gathered for a two-day conversation about big data, the Internet of Things and the economics of personal information.

In closing, I would like to sincerely acknowledge the dedication and teamwork of my staff and the support of my External Advisory Board, as well as the stakeholders in the access and privacy community. Their interest and involvement contribute significantly to the work of this Office. I would also like to respectfully recognize the three Legislative Committees I have worked with over my term: the Select Standing Committee on Finance and Government Services, the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* and the Special Committee to Review the *Personal Information Protection Act*.

I have been honoured to serve as B.C.'s Information and Privacy Commissioner.

Elizabeth Denham
Information and Privacy Commissioner for British Columbia

OUR WORK

Commissioner

The Information and Privacy Commissioner, an independent Officer of the Legislature, oversees the information and privacy practices of public bodies and private organizations in British Columbia. She has the legal authority to investigate programs, policies or information systems in order to assess compliance with B.C.'s access and privacy laws. The Commissioner also investigates complaints, reviews appeals of access to information responses, comments on the implications of new programs, policies, and technologies on access and privacy rights and engages in public education and outreach activities.

In 2015-16, the Commissioner and her staff received 9,024 files, an increase of 7% over last year.

Information Services

Intake Officers help individuals seeking a review of an access to information request or filing a complaint. This includes screening, determining issues and providing assistance to individuals to complete related forms and letters and initiating appropriate action. Intake Officers are also first responders to breach notifications and can assist in the early resolution of complaints.

In 2015-16, Intake Officers received 154 privacy breach notifications, an increase of almost 17% over the previous year. There were 5,737 requests for information, an increase of almost 10% over the previous year.

Investigation & Mediation

Complaints and appeals of access to information requests are assigned to OIPC Investigators, who review the facts and any records at issue and work with the complainant and the public body to reach a resolution.

In 2015-16, more than 99% of all complaints were resolved without a formal hearing or inquiry: no change over 2014-15.

Adjudication

When a complaint or review cannot be resolved between the parties, the Commissioner or her delegate will conduct a formal inquiry. Adjudicators assess the evidence and arguments of parties and issue final and binding decisions that have the force of law. Orders can be appealed to the B.C. Supreme Court.

In 2015-16, the Office issued 81 orders, an increase of 22% over the previous year.

Policy & Technology

Policy Analysts research and analyze current and emerging access and privacy issues, conduct systemic investigations, review and comment on privacy impact assessments and consult with public bodies and private organizations. They also review and analyze proposed legislation with an eye to the implications for access and privacy rights of British Columbians.

In 2015-16, 187 policy or issue consultation files were opened by Policy Analysts, an increase of almost 10% over the previous year.

Audit & Compliance

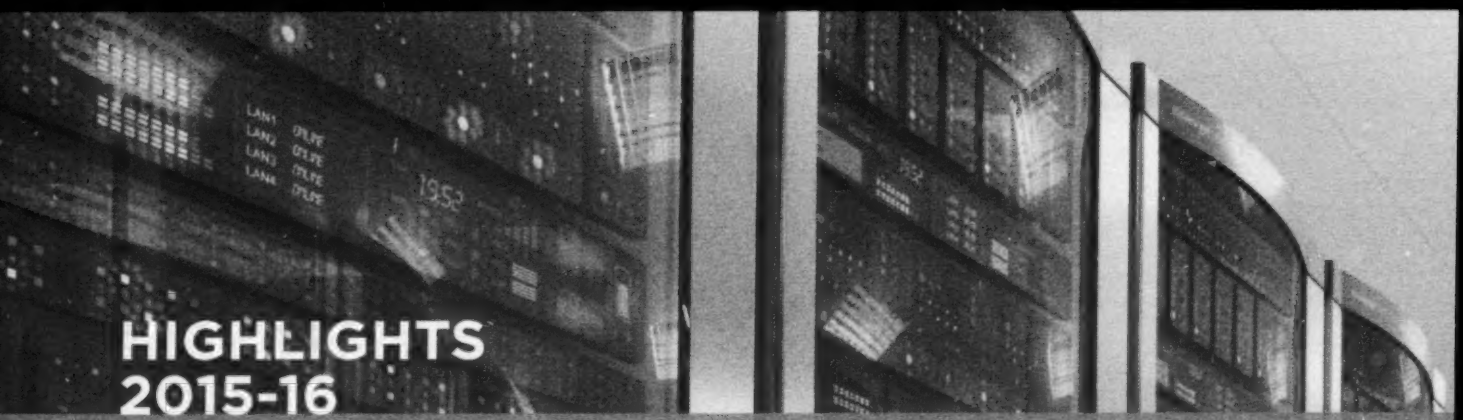
The Audit & Compliance team proactively assesses the extent to which public bodies and private sector organizations protect personal information and comply with access provisions under the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*.

In September 2015, the Commissioner published the OIPC's second audit report, *Examination of British Columbia Health Authority Privacy Breach Management*, conducting audits across all eight of the province's health authorities.

Communications

The Communications team helps publicize the Commissioner's work and engages in public education and outreach to inform and empower individuals to exercise their information and privacy rights. The Office's website, social media presence, media relations, corporate reporting and open data/ proactive disclosure all fall under the Communication department's oversight.

In 2015-16, the Communications team fielded 286 media requests, an increase of 9% over the previous year.



HIGHLIGHTS 2015-16

Commissioner Investigates Access to Information Practices

A high profile investigation by the Commissioner identified major deficiencies in the access to information practices of two British Columbia government ministries and the Office of the Premier, including negligent searches for records, a failure to keep adequate email records, a failure to document searches and the willful destruction of records responsive to an access request.

READ: *Access Denied, page 16.*

DOWNLOAD: *Access Denied: Record Retention and Disposal Practices of the Government of British Columbia* (oipc.bc.ca).

Freedom of Information and Protection of Privacy Act (FIPPA) Reviewed

The OIPC participated in a comprehensive review of the province's public sector legislation, undertaken by an all-party Special Committee of the Legislature.

READ: *FIPPA Review,* page 14.

DOWNLOAD: *Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act* (oipc.bc.ca).

Annual Privacy and Access Conference Held in Vancouver

In November 2015, the OIPC welcomed 332 delegates to Vancouver for the second "Privacy and Access 20/20: The Future of Privacy" conference. The two-day event offered thought-provoking content from experts in industry, government and civil society and showcased speakers from B.C. as well as national and international thought leaders. Topics included youth privacy and cyberbullying, big data, cultures of privacy, wearable technologies, surveillance and national security issues, the connected car and the age of robotics.

OIPC Nominated for Role of Secretariat for Asia-Pacific Privacy Authorities (APPA)

The OIPC was nominated in December 2015 for the role of Secretariat for APPA. The privacy regulators from 19 Pacific Rim countries meet twice each year to form partnerships and collaborate on privacy enforcement. The OIPC will assume this role in July 2016 for a three-year term.

OIPC Partners in Big Data Surveillance Study

The OIPC became a project partner with four universities across Canada in a five-year study of big data surveillance, funded by a $2.5 million research grant from the Social Sciences and Humanities Research Council of Canada (SSHRC).

READ: *Big Data Surveillance Study,* page 22.

GPEN Regulators Conduct Sweep of Children's Websites

In September 2015, 29 privacy regulators took a close look at nearly 1,500 popular children's websites and apps to assess how much personal information was being collected — and what privacy policies and controls were in place to protect that information. In its review of 100 North American social media, gaming and educational websites and apps, the OIPC found that many failed to explain, in child-friendly terms, what personal information was being collected, or how it might be shared. The OIPC wrote to the operators of the websites and apps that caused concern, communicating changes that the Commissioner expected them to make.

HIGHLIGHTS 2015-16

Commissioner Investigates Ministry of Education Breach

Following an investigation, the Commissioner found that the Ministry of Education failed to protect the personal information of 3.4 million B.C. and Yukon students. The records, some of which contained highly sensitive personal information, had been stored more than four years ago on an unencrypted portable hard drive which the Ministry could not locate. Given the passage of time, the main goal of this report was to highlight lessons from the past to help prevent future breaches. In her findings, the Commissioner underscored the importance of executive leadership and privacy management programs and made nine recommendations to strengthen the security of personal information maintained by the Ministry.

DOWNLOAD: *Ministry of Education Investigation Report* (oipc.bc.ca).

Mount Polley Report Redefines Duty to Inform

The Commissioner examined whether government had a duty to release information about the Mount Polley tailings pond breach. The report also reinterpreted s. 25(1)(b) of FIPPA. The Commissioner determined that urgent circumstances are no longer required in order for there to be a finding that the disclosure of information is clearly in the public interest.

READ: *In the Public Interest*, page 18.

DOWNLOAD: *Review of the Mount Polley Mine Tailings Pond Failure and Public Interest Disclosure by Public Bodies* (oipc.bc.ca).

Commissioner Examines Health Authority Privacy Breach Management Policies

The Commissioner published a report calling for immediate action to address gaps in the privacy breach management practices of B.C.'s health authorities. Strong policies, compliance monitoring, and training of health care providers and staff are essential to maintaining the privacy rights of the citizens of B.C. The Commissioner made 13 recommendations for immediate preventative action to help protect the highly sensitive personal information health authorities collect, use and store.

DOWNLOAD: *Examination of British Columbia Health Authority Privacy Breach Management* (oipc.bc.ca).

Continuous Improvement Project Launched

The number of requests for information and appeals received by the OIPC continues to increase annually. As a result, the Office has a backlog of complaints and reviews. In early 2015, the Office initiated a Continuous Improvement Project ("CIP") to increase efficiencies in the Office's intake and investigation processes. The goal is to close files faster while maintaining administrative fairness and a high level of public service. The Office implemented the improvements in October 2015.

OIPC Rules on Metadata from Government and Public Sector Entities

An applicant requested information about the email addresses and date and time of emails sent and received on servers responsible for the email traffic for B.C. Government and other public sector entities. A Ministry refused to disclose the record on the basis that it would be an unreasonable invasion of privacy under s. 22. An OIPC Adjudicator found that s. 22 did in fact apply and that it was also unreasonable under s. 4(2) for the Ministry to sever personal information and disclose the remaining information to the applicant.

DOWNLOAD: *Order F15-63* (oipc.bc.ca).

Joint Cyberbullying Report with the Representative for Children and Youth

The Commissioner and the Representative for Children and Youth released a joint report on cyberbullying in November 2015. The officers called upon the provincial government to develop a comprehensive, cross-ministry strategy to both prevent and mitigate the effects of cyberbullying. They also recommended that the Attorney General consider developing prosecution guidelines for the application of criminal law that best reflected a child-centred approach. In addition, they recommended that the Ministry of Education ensure that learning objectives about cyberbullying and digital citizenship are part of the re-designed B.C. provincial curriculum, that teachers receive professional development on the subject, and that cyberbullying be incorporated into mandatory school codes of conduct.

DOWNLOAD: *Cyberbullying: Empowering Children and Youth to be Safe Online and Responsible Digital Citizens* (oipc.bc.ca/special-reports).

COMPLIANCE SUMMARY

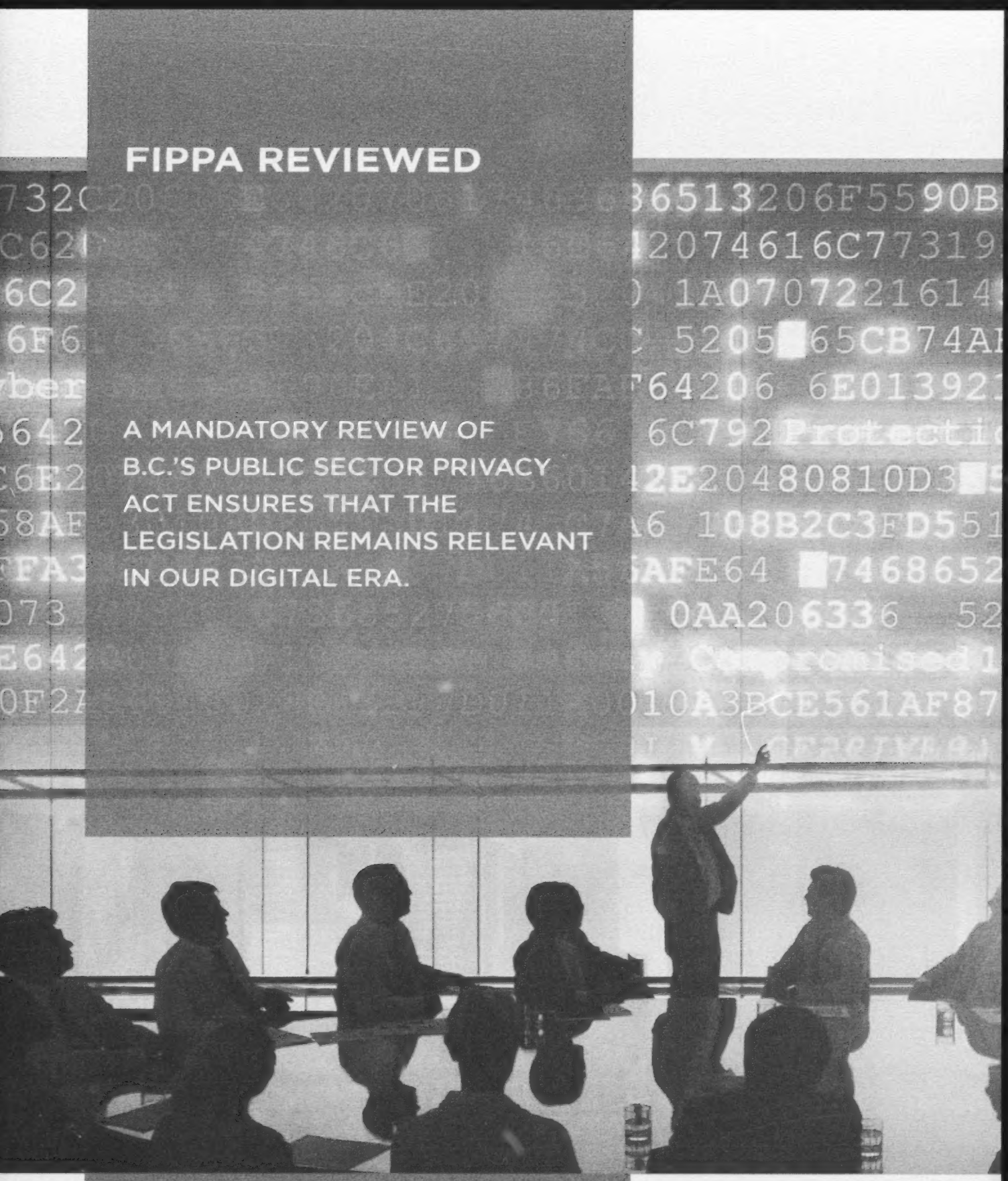
SUMMARY OF COMPLIANCE FOR OIPC SPECIAL AND INVESTIGATION REPORTS 2015-16

INVESTIGATION/SPECIAL REPORT	STATUS
July 2, 2015 *Review of the Mount Polley mine tailings pond failure and public interest disclosure by public bodies.*	The OIPC made specific recommendations to the Ministries of Environment and Energy and Mines, as well as recommendations to the wider public sector. The Ministry of Energy and Mines is working with the Privacy Compliance and Training Branch of the Ministry of Finance to understand and apply the new interpretation of Section 25(1)(b) as set out in the Investigation Report. The Ministry of Environment reviewed our recommendations and determined that it did not have information regarding the Mount Polley tailings pond failure that met the threshold for disclosure under s. 25(1)(b). Our Office continues to support the public sector through consultations and workshops to help them understand what is required to comply with s. 25 of FIPPA.
September 30, 2015 *Examination of British Columbia Health Authority Privacy Breach Management*	Each of the health authorities has taken steps toward implementation of the Commissioner's 13 recommendations, many in the areas of providing mandatory privacy training to staff and conducting physical site audits of privacy and security safeguards. In addition, the Health Information Privacy and Security Operations Committee (made up of privacy officers from each authority) has undertaken collaborative work to establish a common framework for classifying and counting breaches. In sum, more effort is needed to regularly conduct compliance monitoring activities, including analyzing and reporting out on the breaches that occur within their organizations to identify the root causes of breaches and to determine and implement appropriate solutions. The OIPC will continue to work with the health authorities toward full implementation of the recommendations.

INVESTIGATION/SPECIAL REPORT	STATUS
October 22, 2015 *Access Denied: Record Retention and Disposal Practices of the Government of British Columbia*	Government has committed to addressing all of the OIPC's recommendations. Some, such as "releasing records responsive to requests," were promptly implemented. Government hired and accepted the advice of former Commissioner David Loukidelis regarding how to implement several other OIPC recommendations. Government also referred other recommendations for legislative reform to the Select Standing Committee to Review the Freedom of Information and Protection of Privacy Act. The Committee supported these reforms and recommended adding a legislated duty to document FIPPA, providing independent oversight over allegations of unauthorized records-destruction and introducing an offence for destroying records with the intention of denying access rights. The OIPC will continue to work with government to ensure the Access Denied recommendations are fully implemented.
November 13, 2015 *Cyberbullying: Empowering children and youth to be safe online and responsible digital citizens*	An inter-ministerial "working group and advisory body" on cyberbullying was developed in Dec. 2015 with representation from the Ministry of Education, the Ministry of Justice, the Ministry of Child and Family Development and the Office of the Representative for Children and Youth. Its mandate is to inform the development of a draft plan to respond to the recommendations. The body will draft a strategic plan to share with the Representative and Commissioner in 2016. The recommendation that a single point of accountability be identified in government remains unaddressed; to date no progress has been made on the other recommendations.
January 28, 2016 *Ministry of Education (lost portable hard drive)*	The Ministry of Education has accepted the OPIC's nine recommendations. It has completed some of the recommendations and is actively working on the others. It is updating the OIPC with its progress as it works through each recommendation.

FIPPA REVIEWED

A MANDATORY REVIEW OF B.C.'S PUBLIC SECTOR PRIVACY ACT ENSURES THAT THE LEGISLATION REMAINS RELEVANT IN OUR DIGITAL ERA.



When the *Freedom of Information and Protection of Privacy Act* ("FIPPA") first came into effect in 1993, the internet, email and online data collection were still relatively new. But over the past 22 years, digital technology has had a profound impact on how government manages information and records.

Fortunately, regular reviews are mandated for the public privacy and access laws. Every six years, a Special Committee undertakes a comprehensive review of FIPPA to determine its effectiveness, given the current environment. The latest review began in July 2015. For the better part of a year, the Committee consulted the public, government and the OIPC and developed recommendations to ensure that the Act keeps up with our technologically driven world.

According to Elizabeth Denham, Information and Privacy Commissioner, changes in the external environment make reviews of the legislation very important. "The Committee has made 39 recommendations, which, if implemented, will strengthen access to information and privacy rights in B.C. and make our laws more consistent with other jurisdictions."

The Commissioner is particularly pleased that the Committee is recommending a legislated duty to document for public bodies. "Access rights depend on the creation of appropriate public records that document the key decisions and activities of government. If those records are absent, public accountability is lost, trust erodes and, ultimately, the public's access to information is denied," she says. "Should government and the legislature accept the Committee's recommendations, British Columbia will be in a leadership position as the first jurisdiction in Canada to bring into force a statutory duty to document."

When there are allegations that a record has been destroyed, the public's trust is diminished. For this reason, independent oversight of allegations of destruction is essential to maintain the public's trust and confidence in the freedom of information process. To this point, the Committee recommended an expansion of the Commissioner's oversight to review allegations of unauthorized destruction of records, as well as the addition of a fine of up to $10,000 for destroying, altering, or concealing a record with the intention of denying access rights under FIPPA.

In addition, the Committee also recommended mandatory breach notification for the public sector. "In most cases the public has no choice but to hand over their most sensitive information to government," says Commissioner Denham "We have to trust that government will protect personal information from potential threats."

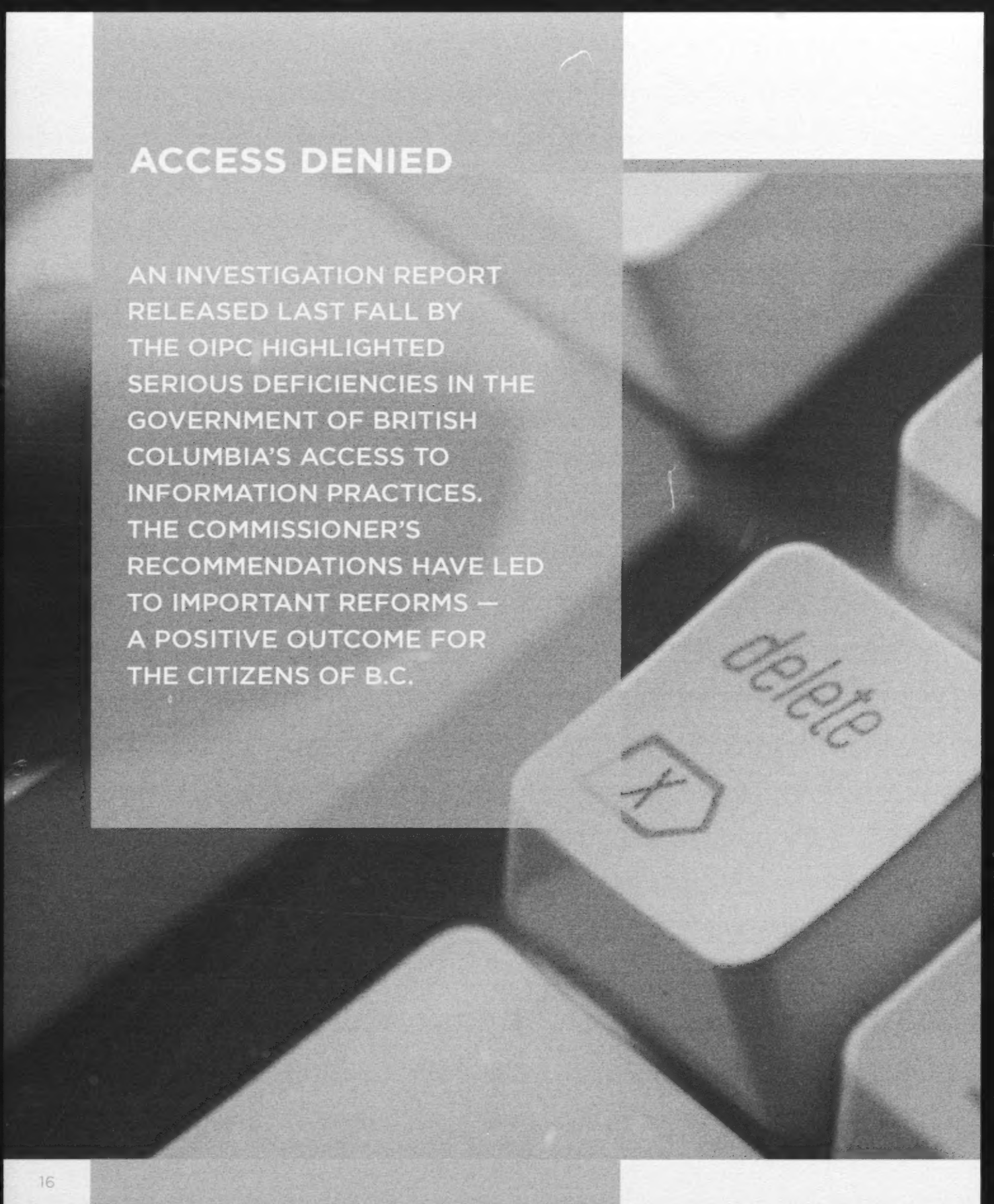
Mandatory breach notification alerts individuals to potential harms as a result of a breach, and gives them an opportunity to take measures to protect themselves, she adds. "If implemented, this recommendation will result in B.C. being current with legislated breach notification in other jurisdictions.

"I would like to thank the Committee members and staff for their thorough and thoughtful work and express appreciation to everyone who participated in this process. I look forward to government's response." ■

DOWNLOAD: The Report of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* (https://www.leg.bc.ca/parliamentary-business/committees/40thparliament-5thsession-foi/)

ACCESS DENIED

AN INVESTIGATION REPORT RELEASED LAST FALL BY THE OIPC HIGHLIGHTED SERIOUS DEFICIENCIES IN THE GOVERNMENT OF BRITISH COLUMBIA'S ACCESS TO INFORMATION PRACTICES. THE COMMISSIONER'S RECOMMENDATIONS HAVE LED TO IMPORTANT REFORMS — A POSITIVE OUTCOME FOR THE CITIZENS OF B.C.



The digital era has radically altered the way we create, use and store information. Where government records were once stored by file clerks in paper file folders and metal filing cabinets, today they can be stored by any government employee, in any number of places, from hard drives, flash drives and smartphones to personal devices, government servers and beyond.

In some cases, records of important business decisions aren't created at all. "The trend toward oral government has seriously hindered modern record keeping," says Commissioner Elizabeth Denham. "The problem is, freedom of information can only be exercised when public bodies create and keep records of the key actions they take and the decisions they make."

The OIPC has long stressed the importance of proper record keeping. But a recent report, *Access Denied: Record retention and disposal practices of the government of British Columbia*, turned an even brighter light onto the issue. One of the most resource-intensive and technical investigations the OIPC has undertaken, it probed complaints about three freedom-of-information requests. One involved the Ministry of Transportation and a whistleblower's allegation that a supervisor intentionally deleted records responsive to an FOI request involving Highway 16/the Highway of Tears.

During the course of the investigation, investigators requested monthly email backups, seized and inspected computers and reviewed mailbox metadata and message tracking logs. The OIPC uncovered negligent searches for records, a failure to keep adequate email records, a failure to document searches and wilful destruction of records responsive to an access request. "Taken together, these practices threaten the integrity of access to information in British Columbia," says the Commissioner, who made 11 recommendations in her report. "Our investigation revealed a clear need for improvements to some of the processes the government employs in responding to freedom of information requests," she says. With its publication in October 2015, the Commissioner also referred part of the file to the RCMP — a first for the office.

Government reacted swiftly to the report, engaging former Commissioner David Loukidelis to provide advice and assistance in implementing Commissioner Denham's recommendations. They then made a number of improvements, including increased training on records management, privacy, and the handling of requests, as well as initiatives to increase timeliness and responsiveness. The position of Chief Records Officer and the responsibility for information access policy and guidance were also shifted to the Ministry of Finance.

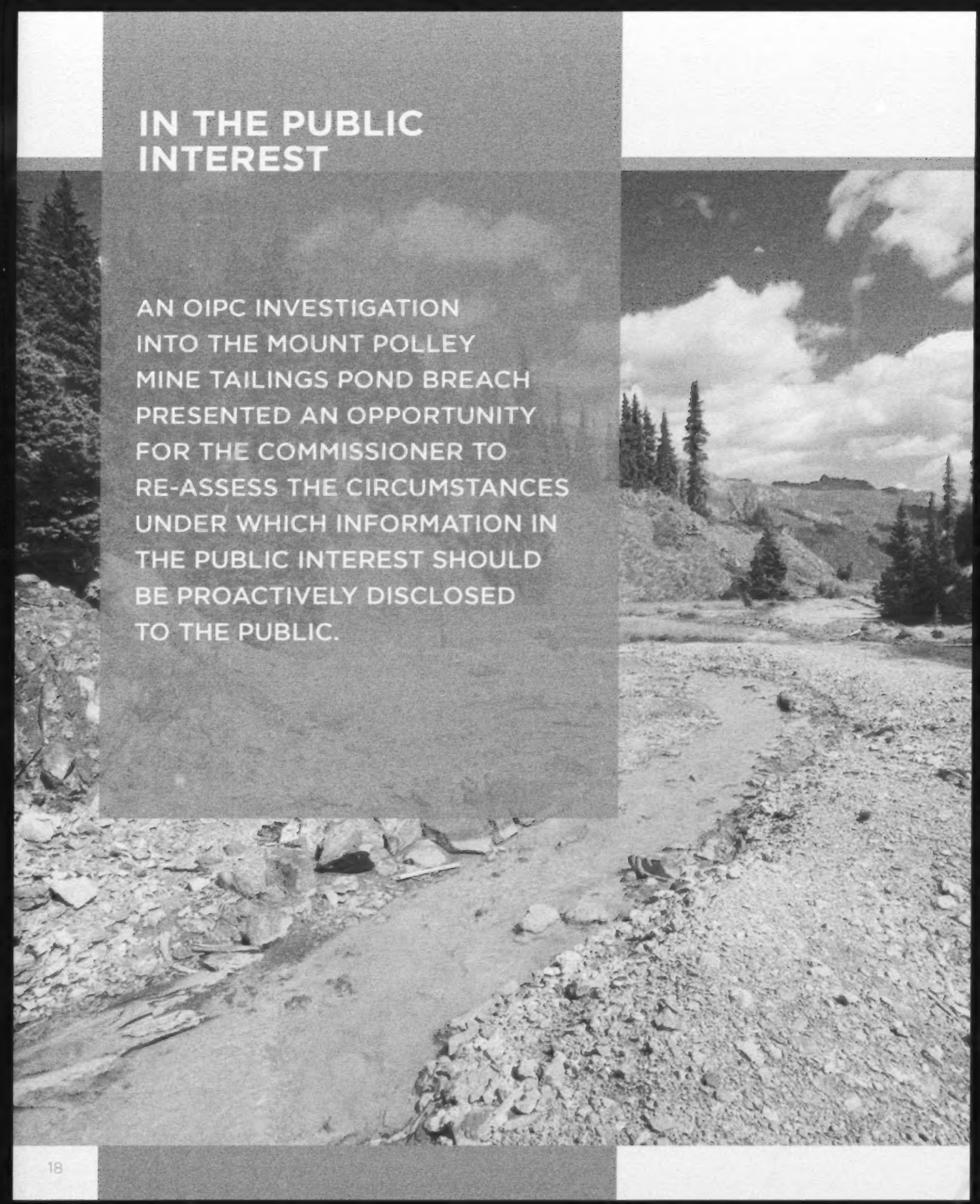
On May 9, 2015, government also announced its intention to significantly expand proactive disclosure. One day later, they brought the *Information Management Act* into force, replacing the Document Disposal Act of 1936 and providing a modern framework for records management within government in the digital age.

"I'm pleased that government listened to these concerns and is enacting meaningful reforms," says the Commissioner. "Proper record keeping is absolutely essential to accountable government, good governance, and freedom of information. Once the province has delivered on all of the announced commitments, British Columbia will resume its position of leadership in Canada in access to information." ■

DOWNLOAD: *Access Denied: Record Retention and Disposal Practices of the Government of British Columbia* (oipc.bc.ca).

IN THE PUBLIC INTEREST

AN OIPC INVESTIGATION INTO THE MOUNT POLLEY MINE TAILINGS POND BREACH PRESENTED AN OPPORTUNITY FOR THE COMMISSIONER TO RE-ASSESS THE CIRCUMSTANCES UNDER WHICH INFORMATION IN THE PUBLIC INTEREST SHOULD BE PROACTIVELY DISCLOSED TO THE PUBLIC.



It was one of this province's worst environmental disasters. On August 4, 2014, the tailings pond at the Mount Polley mine in the Cariboo Region failed, breaching the pond's perimeter embankment and releasing 25 million cubic metres of water and effluent into Polley Lake, Hazeltine Creek and Quesnel Lake. Government initiated three separate investigations to determine the cause of the tailings pond dam failure. After receiving complaints that alleged that government had information about the incident that it should have disclosed to the public, the Commissioner also initiated an investigation. Her main emphasis, however, was on public interest and the duty to inform.

The *Freedom of Information and Protection of Privacy Act* requires public bodies to proactively disclose information to the public in two instances: one, where there is a risk of significant harm to the environment, health or public safety; and two, where disclosure is, for any other reason, clearly in the public interest.

In this investigation report, Commissioner Denham analyzed how both tests applied to the facts in Mount Polley. She concluded that government did not have information in its possession that disclosed a risk of significant harm to the environment or to the health and safety of the public. However, the Commissioner used the opportunity to reassess the circumstances in which proactive disclosure would be "clearly in the public interest."

"In a prior report on section 25, I expressed the view that public interest disclosures should not require urgent circumstances; such a requirement effectively undermines the purposes of the legislation. My investigation of the Mount Polley mine tailings pond breach presented the opportunity to examine this issue in depth," she says.

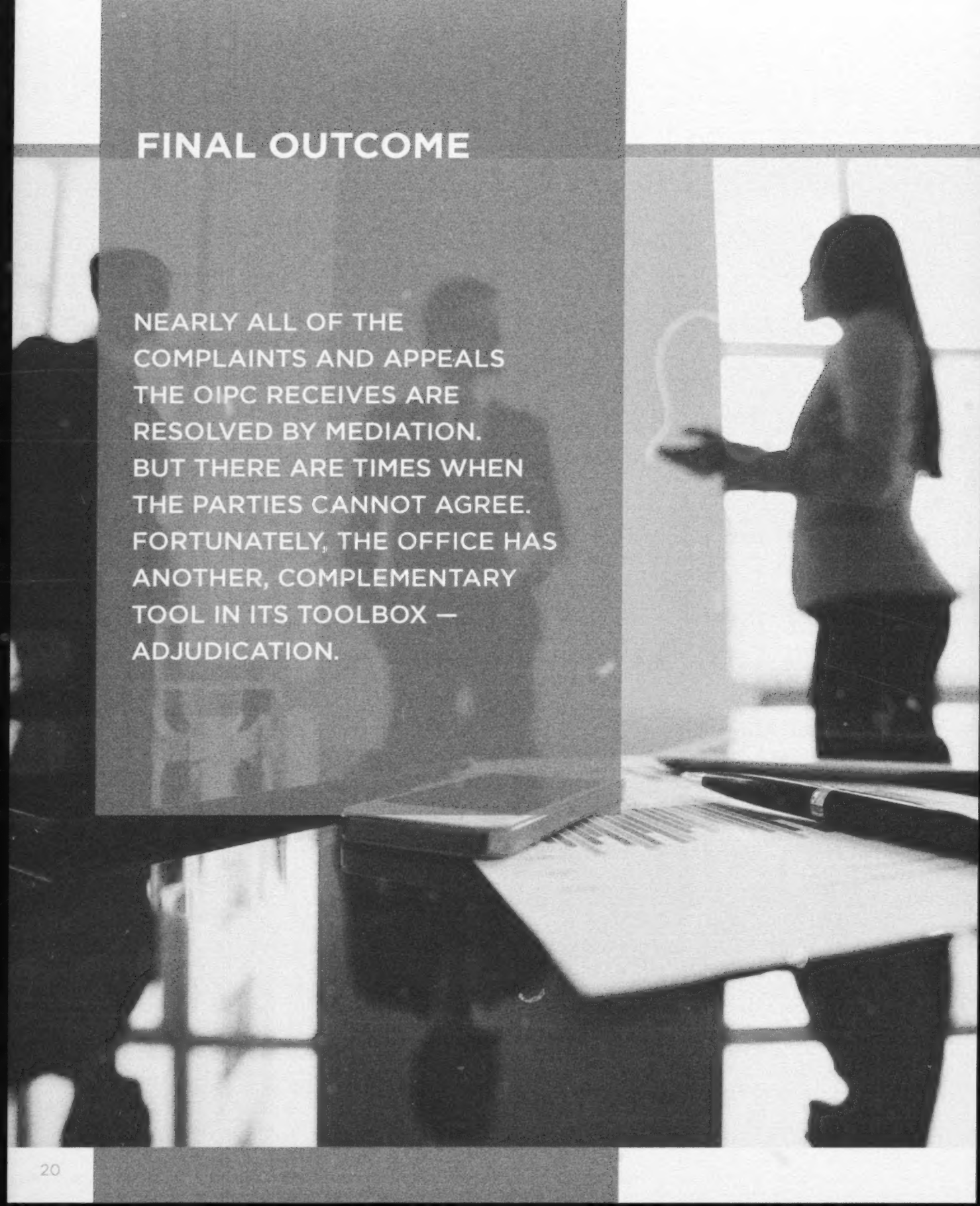
The Commissioner concluded that urgent circumstances are no longer required to trigger proactive disclosure where there is a clear public interest in disclosure of the information. "This returns the section to a plain-language reading of what I have determined to be the intention of the Legislature in its enactment of this section of FIPPA," says Denham.

In light of the re-interpretation of s. 25(1)(b) presented in the investigation report, the Commissioner recommended that the Ministries of Energy and Environment promptly and diligently consider what information, if any, must be disclosed in the public interest specific to the Mount Polley mine tailings pond breach.

"With the publication of this report, it is incumbent upon all public bodies to evaluate their policies for disclosure pursuant to s. 25(1)(b) of FIPPA, and to promptly re-evaluate whether they currently have information that should be proactively disclosed as clearly in the public interest as described in this report. This may include information that is currently the subject of an access to information request," says Denham. ■

DOWNLOAD: *Review of the Mount Polley mine tailings pond failure and public interest disclosure by public bodies* (oipc.bc.ca).

FINAL OUTCOME



NEARLY ALL OF THE COMPLAINTS AND APPEALS THE OIPC RECEIVES ARE RESOLVED BY MEDIATION. BUT THERE ARE TIMES WHEN THE PARTIES CANNOT AGREE. FORTUNATELY, THE OFFICE HAS ANOTHER, COMPLEMENTARY TOOL IN ITS TOOLBOX — ADJUDICATION.

Mediation is a time-honoured method of resolving conflicts quickly and efficiently. It's also a tool the OIPC's team of investigators use on a daily basis as they seek fair and expeditious resolutions for requests for review that are brought to this office.

But if mediation cannot produce a satisfactory outcome, any party (applicant, complainant, third party, public body, or organization) can request an inquiry or hearing that leads to a binding order. Their complaints are sent to the OIPC's skilled team of adjudicators, or to the Commissioner, who has order-making powers under both the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and the *Personal Information Protection Act* ("PIPA").

"These powers are essential for my effective performance," says the Commissioner. "They help me ensure that private sector organizations (governed by PIPA) and public bodies (governed by FIPPA) fulfill their responsibilities and are aware of the consequences of inertia or carelessness."

The adjudication process follows a prescribed series of steps. First, the investigator who mediated the dispute must grant the request for an inquiry. Then she or he will draw up a Fact Report and a notice of the issues that resulted in the matter being brought to our office. Aside from these documents, the person conducting the inquiry (the Commissioner or a delegated adjudicator) will have no knowledge of anything that transpired during the mediation phase.

Next, the OIPC invites parties to the dispute to make submissions to the inquiry. Other individuals, such as potentially affected third parties or interveners, may be invited as well. The adjudicator analyzes the facts, issues, and application of the law, and then provides a rationale for the legally binding written order. All orders are posted on our website following their release.

During the 2015-16 fiscal year the Commissioner and her team of adjudicators published 81 orders, an increase of more than 20% over 2014-15. Though each order deals with a unique set of circumstances, they are often precedent setting, as was the case with Order F15-23. It was the first to extensively examine and interpret whether FIPPA authorizes public bodies to withhold portions of records as non-responsive or out of scope of the request. The adjudicator concluded that FIPPA does not authorize a public body to withhold information from a record on the basis that the information is not responsive.

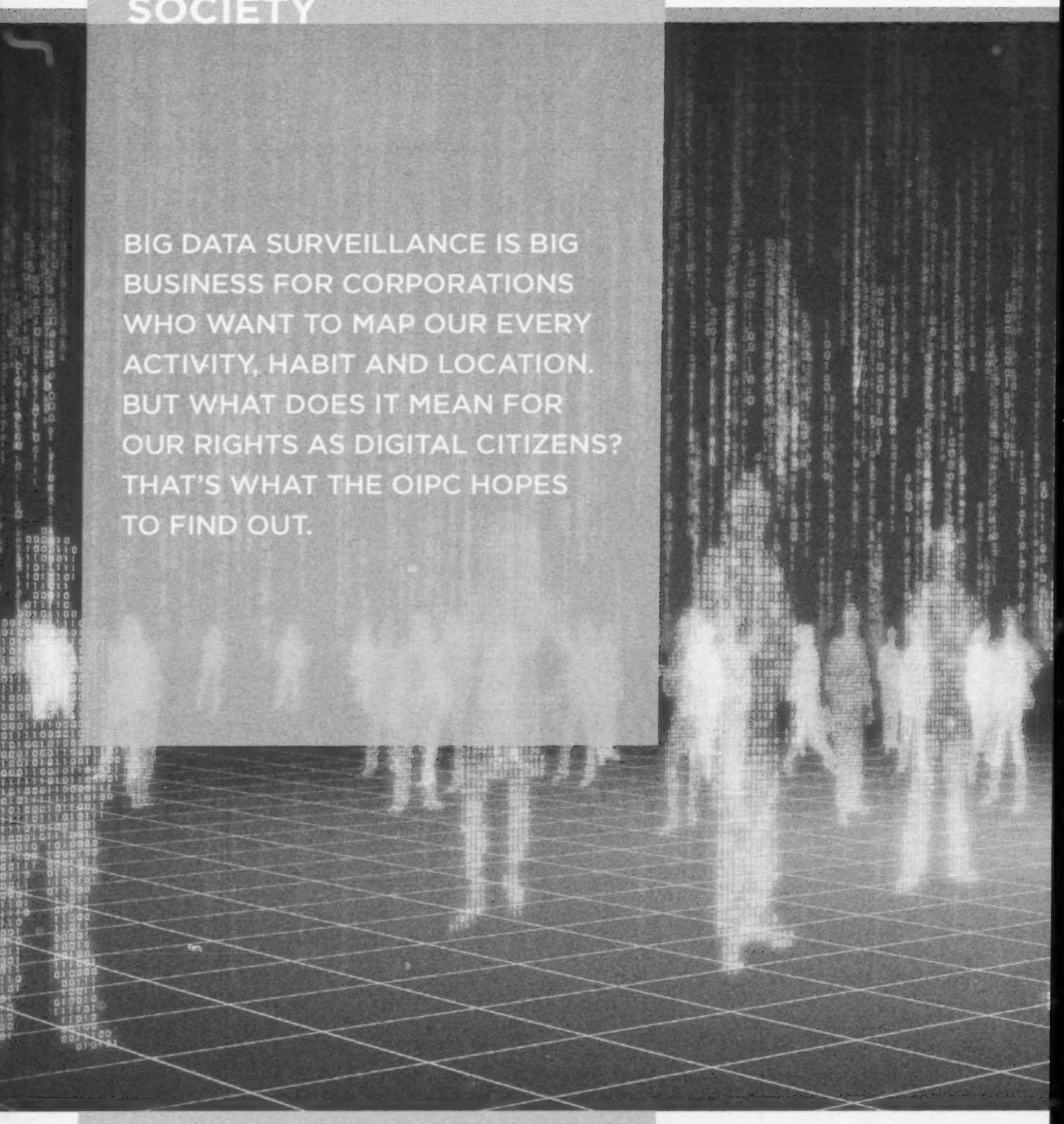
Orders often reflect issues that are trending in other OIPC investigations, such as the sensitivity of health care records. With Order F15-57, the Commissioner found that the Ministry of Children and Family Development disclosed two records that contained the personal information of the complainant and her family in the course of its review of the handling of the complainant's case with the Ministry. The Commissioner also found that this disclosure was authorized by s. 33.2(c) of FIPPA, as it was to employees of the Ministry, and necessary for the duties of those employees. Finally, the Commissioner found that the security arrangements made by the Ministry for the conduct of its review met its obligation, pursuant to s. 30 of FIPPA, "to make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

Regardless of the outcome, adjudication is important because it allows applicants to exercise their democratic right to information and protection of privacy rights, says Commissioner Denham:

"When these rights are not sufficiently respected, a regulator needs a diversity of tools to ensure compliance with the law," she says. "Adjudication is the right tool to ensure compliance with the law." ■

READ: Learn more about adjudication (oipc.bc.ca).

SURVEILLANCE SOCIETY



BIG DATA SURVEILLANCE IS BIG BUSINESS FOR CORPORATIONS WHO WANT TO MAP OUR EVERY ACTIVITY, HABIT AND LOCATION. BUT WHAT DOES IT MEAN FOR OUR RIGHTS AS DIGITAL CITIZENS? THAT'S WHAT THE OIPC HOPES TO FIND OUT.

Big data uses complex algorithms to match, sort, analyze and categorize large volumes of data. It can identify patterns and is used as a predictive tool. For these reasons, it is undoubtedly valuable for businesses in their decision-making. But the impact of big data surveillance on our privacy rights is unclear, at least for now.

As a project partner in a study of big data surveillance, the OIPC hopes to gain a better understanding of what big data collection and use means to the citizens of British Columbia. The five-year study, made possible by a $2.5 million research grant from the Social Sciences and Humanities Research Council of Canada ("SSHRC"), is being led by Dr. David Lyon, Director of the Queen's University Surveillance Studies Centre. It will examine vulnerabilities generated by big data surveillance in areas such as law enforcement, political parties, and the broader public sector.

"Citizens have questions about how police, political parties, and governments use big data in areas that touch their lives. This project will probe big data surveillance and analyze its scope, effectiveness, and implications," says Commissioner Elizabeth Denham.

The study unites national and international academic institutions, the OIPC, the Office of the Privacy Commissioner of Canada and civil liberty organizations. One of the OIPC's roles in the project is to provide feedback on the direction of the academic research. The OIPC also plans to use the research results to educate and inform the public about privacy issues, conduct investigations and call for reforms of privacy and access laws.

The OIPC has identified five areas for research: big data in government, access to information and transparency, data localization, big data surveillance in the employment arena and the efficacy of big data analytics.

"I want to be able to explain to citizens how these technologies work, so we can focus on our role as a regulator," explains the Commissioner. "I also want to be able to map big data surveillance against Canadian privacy laws."

Perhaps most importantly, the OIPC hopes to translate surveillance functions into real-life impacts on citizens. "Our greatest success in policy and law reform comes when we can convince legislators and the general public why they should care about these issues," she says. "In challenging surveillance and predictive analytics from a privacy perspective, we must give real-life examples and scenarios describing how citizens are affected to answer the question, 'Why should I care?'" ■

DOWNLOAD: More information about the SSHRC research project on big data surveillance (oipc.bc.ca/news-releases/1862).

YEAR IN NUMBERS

In 2015-16, citizens continued to think more about their privacy in all contexts and public bodies and organizations engaged our office more frequently.

Detailed information about the Year in Numbers is presented over the next eight pages. Here is a summary of some of the key findings:

Files Opened

The OIPC opened 9,024 files in 2015-16. In 2014-15, 8,419 files were opened.

+7%

Requests for Information

In 2015-16, the OIPC received 5,737 questions, telephone calls or emails. In 2014-15, 5,200 were received.

+10%

Privacy Breaches

154 privacy breaches were reported to the Office in 2015-16. In 2014-15, 132 breaches were reported.

+17%

Privacy Impact Assessments

48 PIAs were reviewed in 2015-16, compared to 33 PIAs in 2014-15.

+45%

Policy or Issue Consultation

The Office recorded 187 policy/issue consultations in 2015-16, compared to 170 in 2014-15.

+10%

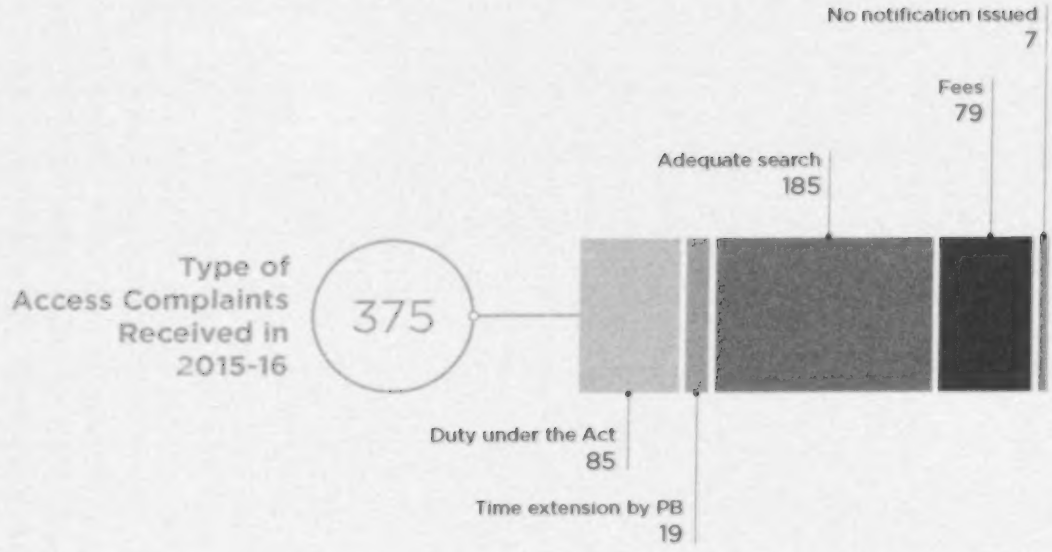
Media Inquiries

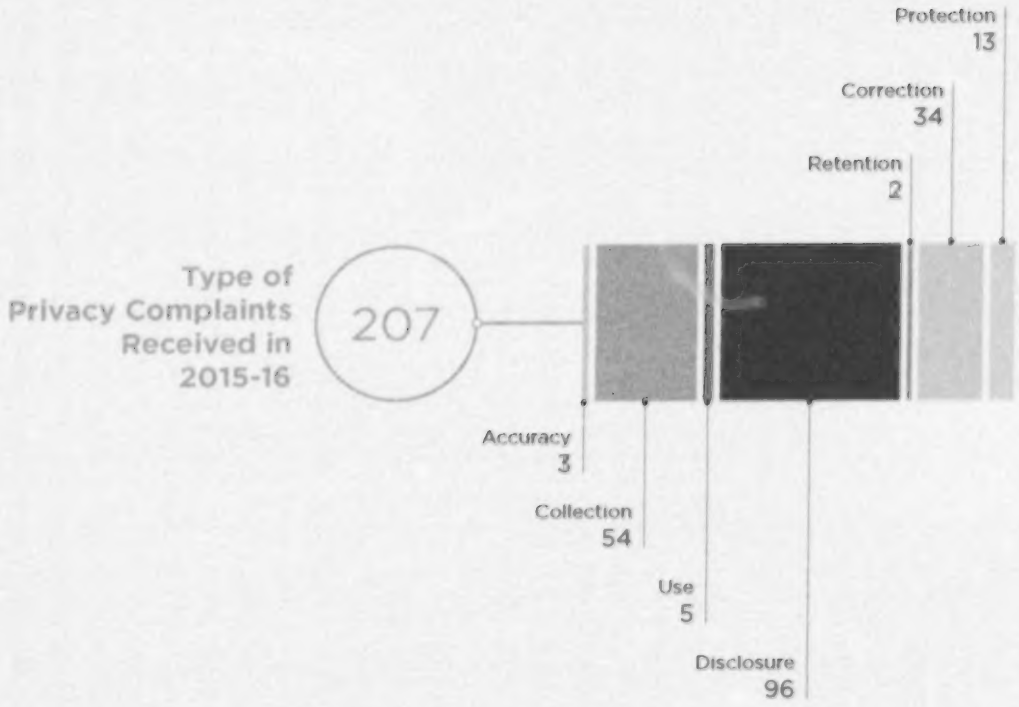
The Office received 286 media requests in 2015-16, compared to 262 in 2014-15.

+9%

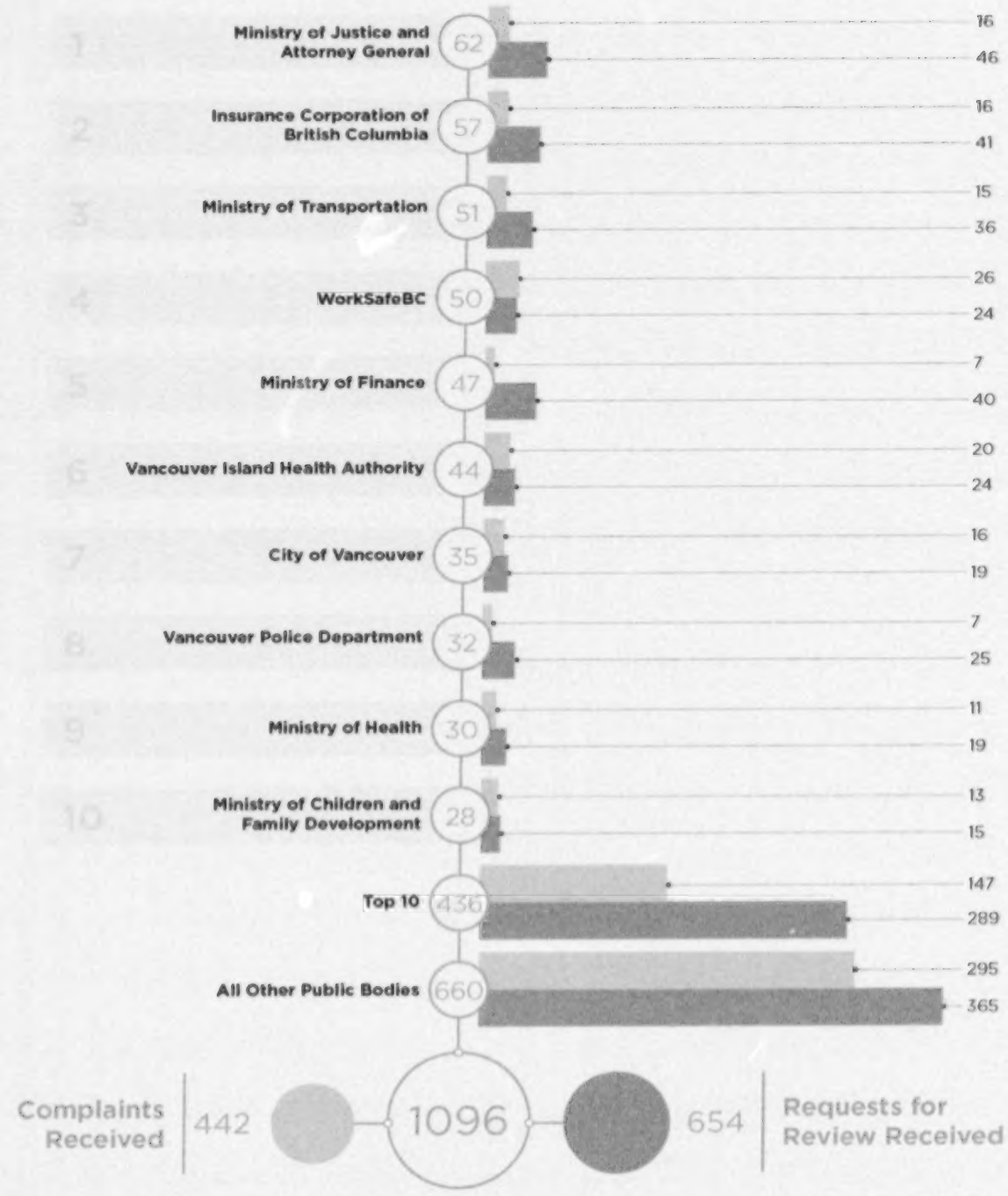
Summary of all FIPPA and PIPA files received in 2015-16

FILE TYPE	Received 2015-16	Received 2014-15	Received 2013-14
Complaints			
Access complaints	375	350	408
Privacy complaints	207	194	231
Requests for review			
Requests for review of decisions to withhold information	710	676	778
Applications to disregard requests as frivolous or vexatious	3	4	7
Time extensions			
Requests by public bodies and private organizations	734	721	853
Requests by applicants seeking a review	7	20	19
Reconsideration of decisions			
Internal reconsideration of OIPC decisions	32	23	27
Adjudication (court review of OIPC decisions)	2	2	2
Information requested			
Requests for information and correspondence received	5,737	5,200	4,024
Media inquiries	286	262	180
FOI requests for OIPC records	16	18	27
Non-jurisdictional issue	11	29	4
No reviewable issue	137	222	165
Files initiated by public bodies and private organizations			
Privacy impact assessments	48	33	20
Privacy breach notifications	154	132	114
Public interest notifications	20	14	17
Policy or issue consultations	197	170	81
Police Act IIO reports	5	19	37
Request for Contact Information (research)	1	1	2
OIPC initiatives			
Investigations	9	8	11
Legislative reviews	43	53	38
Projects	55	87	78
Public education and outreach			
Speaking engagements and conferences	52	67	96
Meetings with public bodies and private organizations	137	107	69
Site visits	0	0	4
Other (section 56 and internal reviews)	56	7	6
TOTAL	9,024	8,419	7,298


Type of Access Complaints Received in 2015-16
375
No notification issued 7
Fees 79
Adequate search 185
Duty under the Act 85
Time extension by PB 19

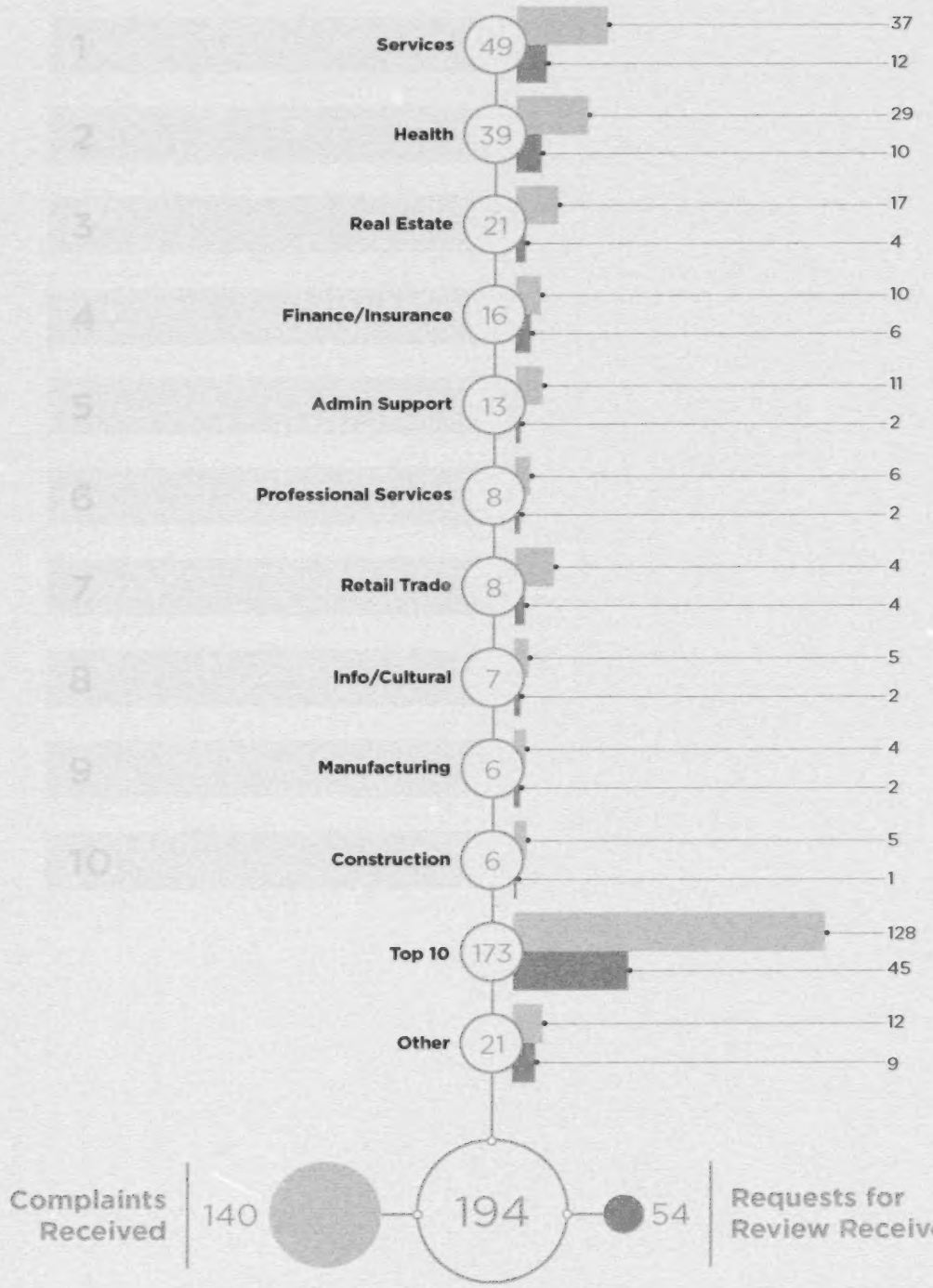

Type of Privacy Complaints Received in 2015-16
207
Protection 13
Correction 34
Retention 2
Accuracy 3
Collection 54
Use 5
Disclosure 96

Number of FIPPA Complaints and Requests for Review Received in 2015-16 by Public Body

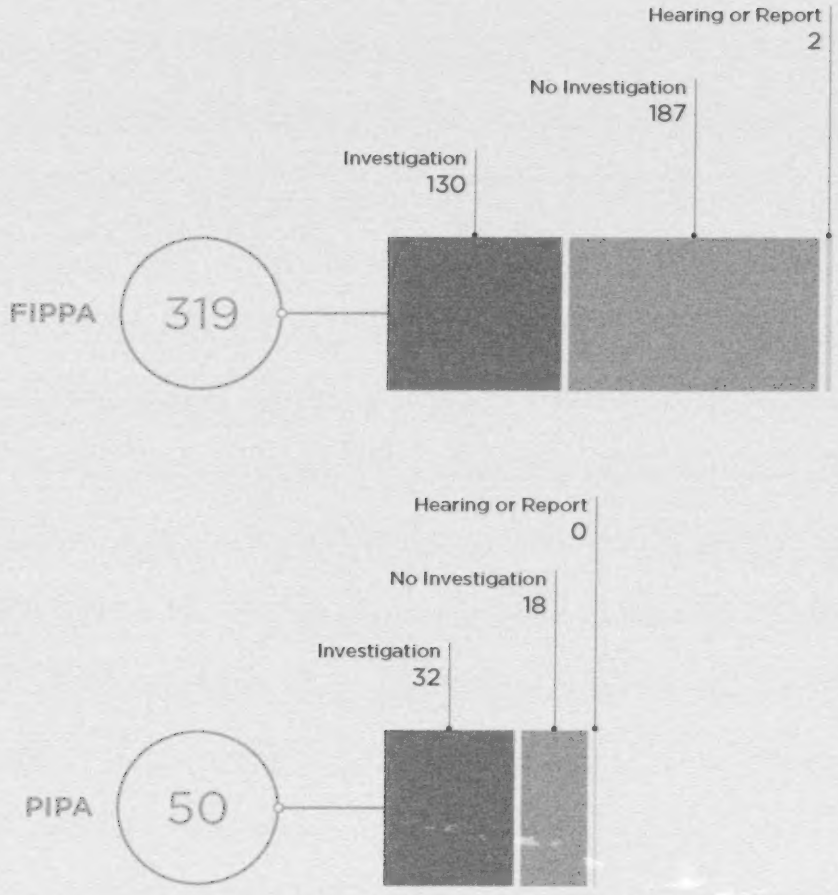


NOTE: The number of requests for review and complaints against a public body is not necessarily indicative of non-compliance, but it may be reflective of its business model or quantity of personal information involved in its activities. The majority of ICBC requests for review, for example, are filed by lawyers performing due diligence on behalf of clients involved in motor vehicle accident lawsuits.

Number of PIPA Complaints and Requests for Review Received in 2015-16 by Sector



Outcome of Access Complaints Resolved in 2015-16

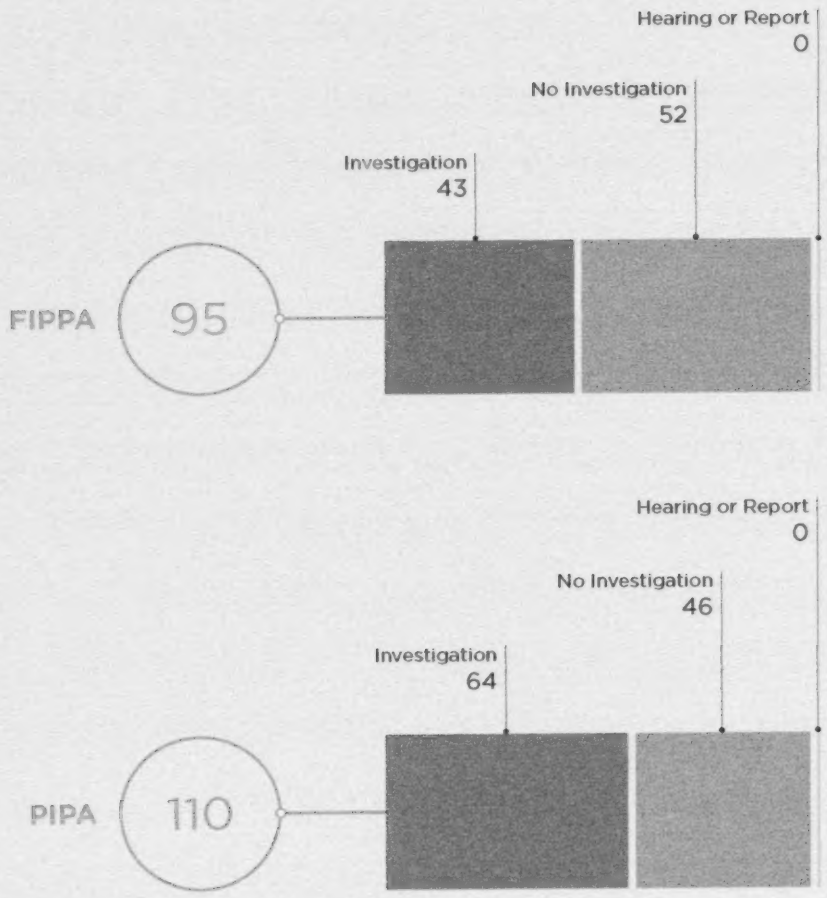


Investigation
Includes files that were mediated, not substantiated, partially substantiated and substantiated.

No Investigation
Includes files referred back to public body, withdrawn, or files the OIPC declined to investigate.

Hearing or Report
Refers to files that proceeded to inquiry and/or a report was issued.

Outcome of Privacy Complaints Resolved in 2015-16

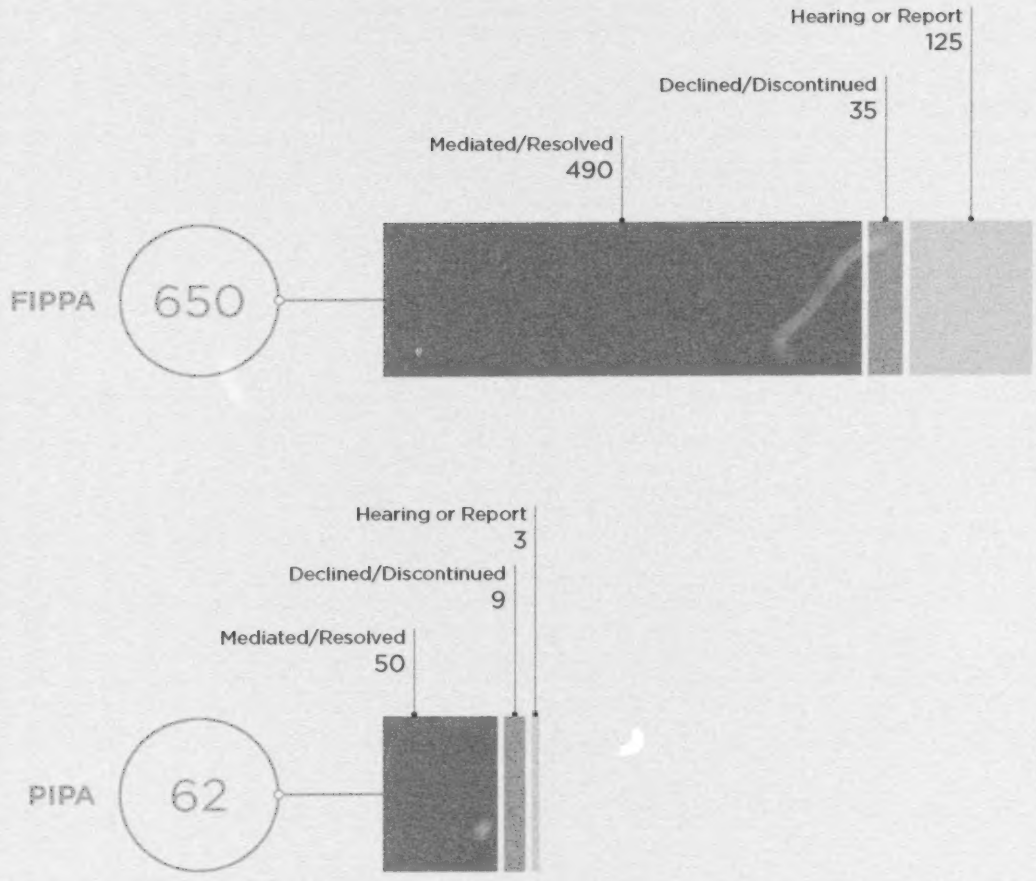


Investigation
Includes files that were mediated, not substantiated, partially substantiated and substantiated.

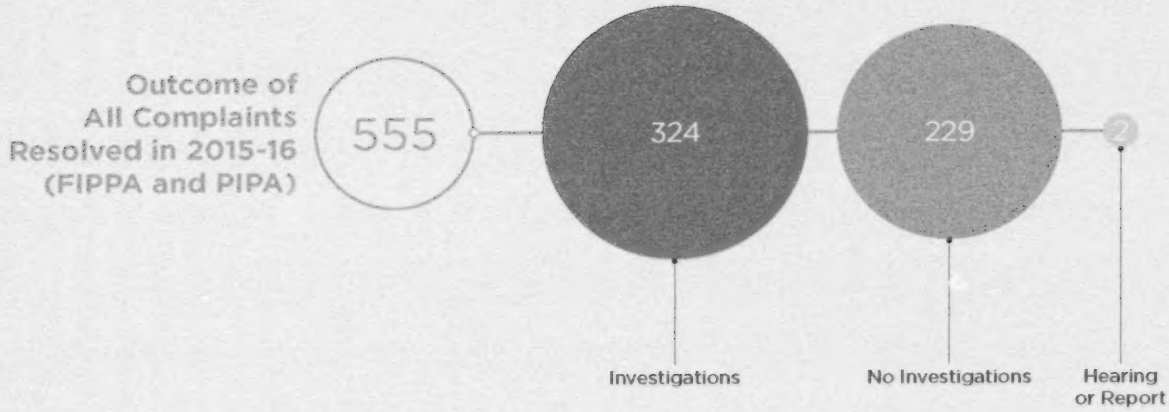
No Investigation
Includes files referred back to public body, withdrawn, or files the OIPC declined to investigate.

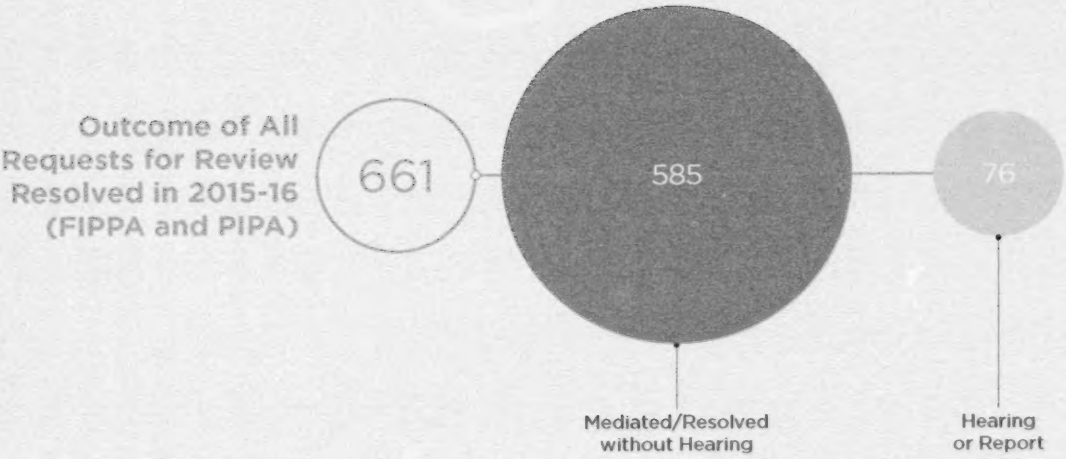
Hearing or Report
Refers to files that proceeded to inquiry and/or a report was issued.

Outcome of Requests for Review Resolved in 2015-16



● **Investigation:** Includes files that were mediated, withdrawn, referred to public body, consent order or other decision by Commissioner.


Outcome of
All Complaints
Resolved in 2015-16
(FIPPA and PIPA)
555
324
229
2
Investigations
No Investigations
Hearing
or Report


Outcome of All
Requests for Review
Resolved in 2015-16
(FIPPA and PIPA)
661
585
76
Mediated/Resolved
without Hearing
Hearing
or Report

FINANCIAL REPORTING

Nature of Operations

The Information and Privacy Commissioner is an independent Officer of the Legislature, whose mandate is established under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and the *Personal Information Protection Act* ("PIPA"). FIPPA applies to more than 2,900 public agencies and accords access to information and protection of privacy rights to citizens. PIPA regulates the collection, use, access, disclosure and retention of personal information by more than 380,000 private sector organizations.

The Commissioner has a broad mandate to protect the rights given to the public under FIPPA and PIPA. This includes: conducting reviews of access to information requests, investigating complaints, monitoring general compliance with the Acts and promoting freedom of information and protection of privacy principles.

In addition, the Commissioner is the Registrar of the Lobbyists Registry program and oversees and enforces the provisions under the *Lobbyists Registration Act*.

Funding for the operation of the Office of the Information and Privacy Commissioner is provided through a vote appropriation (Vote 5) of the Legislative Assembly and through cost recovery from conferences hosted by the Office. The vote provides separately for operating expenses and capital acquisitions, and all payments or recoveries are processed through the Province's Consolidated Revenue Fund. Any unused appropriation cannot be carried forward for use in subsequent years.

As well, part of the Office's funding is dedicated solely for the purpose of carrying out judicial review work, such as proceedings brought against the Office of the Information and Privacy Commissioner. Any portion of the dedicated funding that is unused for that purpose during the fiscal year is returned to the Consolidated Revenue Fund at fiscal year-end.

Accounting Policies and Procedures

This financial reporting has been prepared per the policies and procedures as set out in the Province of British Columbia's Core Policy and Procedures Manual (or "CPPM"), found at: http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm. Section 1.2.4, Governance, Application, describes the entities that are required to follow the CPPM which includes the Office of the Information and Privacy Commissioner.

Voted, Used and Unused Appropriations

The Office receives approval from the Legislative Assembly to spend funds through an appropriation that includes two components — operating and capital. Any unused appropriation cannot be carried forward for use in subsequent years.

The following table compares the Office's voted appropriations, total operating and capital expenses, and the total remaining unused appropriation (unaudited) for the current and previous fiscal year:

	2015/16		2014/15	
	Operating	Capital	Operating	Capital
Appropriation	$5,636,000	$45,000	5,526,000	$45,000
Other amounts	$0	$0	$0	0
	$5,636,000	$45,000	$5,526,000	$45,000
Total appropriation				
Total operating expenses	$5,624,101	-	$5,514,401	-
Capital acquisitions	-	$31,747	-	$16,991
Unused appropriation	$11,899	$13,253	$11,599	$28,009

Tangible Capital Assets

Tangible capital assets are recorded at historical cost less accumulated depreciation. Depreciation begins when the asset is put into use and is recorded on the straight-line method over the estimated useful life of the asset.

The following table shows the Office's capital assets (unaudited):

			2015/16	2014/15
	Closing Cost	Closing Accumulated Amortization	Net Book Value (March 31/16)	Net Book Value (March 31/15)
Computer Hardware and Software	$265,843	-$226,713	$39,130	$28,567
Tenant Improvements	$552,302	-$552,302	$0	$73,640
Furniture and Equipment	$87,749	-$69,007	$18,742	$24,170
Leasehold Commitments	**$905,894**	**-$848,022**	**$57,872**	**$126,377**

Leasehold Commitments

The Office of the Information and Privacy Commissioner has a leasehold commitment with 947 Fort Street Holdings Ltd. for building occupancy costs. Total payments for occupancy costs for the fiscal year 2015-16 were $595,887. Payments to 947 Fort Street Holdings Ltd. for office space for fiscal 2016-17 are estimated to be $613,658.

RESOURCES

Getting Started

- A guide to OIPC processes (FIPPA and PIPA)
- A guide to PIPA for business and organizations
- A guide to FIPPA for individuals
- Early notice and PIA procedures for public bodies

Access (General)

- How do I request records?
- How do I request a review?
- Instructions for written inquiries
- Time extension guidelines for public bodies
- Guidelines for conducting adequate search investigations (FIPPA)

Audit

- Audit and Compliance Program Charter

Privacy Breaches

- Key steps to responding to privacy breaches
- Breach notification assessment tool
- Privacy breach policy template
- Privacy breach checklist

Comprehensive Privacy Management

- Getting accountability right with a privacy management program
- Accountable privacy management in B.C.'s public sector

Privacy (General)

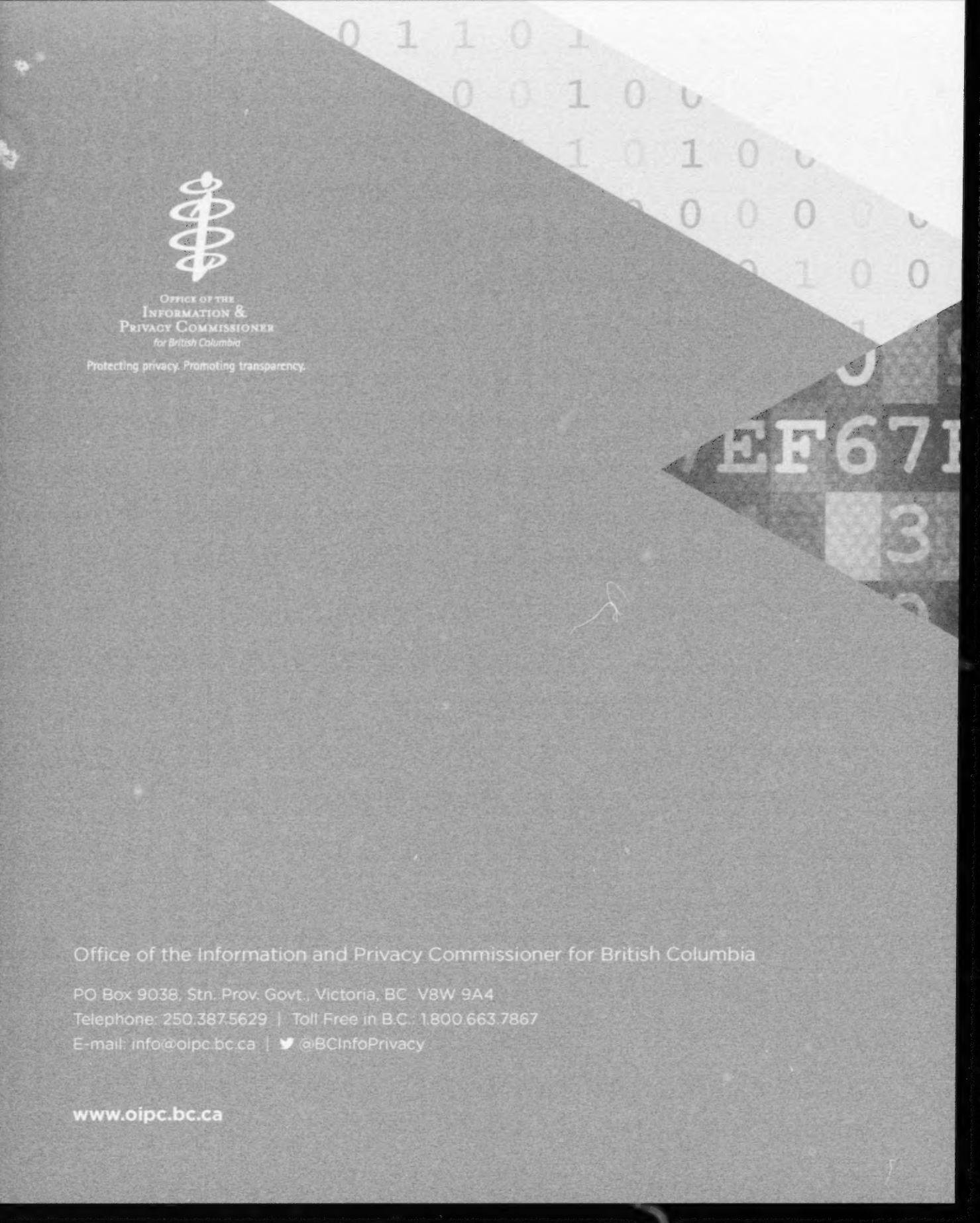
- Guidelines to develop a privacy policy
- Privacy proofing your retail business
- Protecting personal information away from the office
- Identity theft resources
- Privacy guidelines for landlords and tenants
- Privacy emergency kit

Technology & Social Media

- Cloud computing guidelines (public and private sector)
- Good privacy practices for developing mobile apps
- Public sector surveillance guidelines
- Guidelines for overt video surveillance in the private sector
- Use of personal email accounts for public business
- Guidance for the use of body-worn cameras by law enforcement authorities
- Guidelines for online consent
- Guidelines for social media background checks

To request copies of these resources, or to get more information about B.C.'s access and privacy laws, email info@oipc.bc.ca or visit www.oipc.bc.ca

Office of the Information & Privacy Commissioner
for British Columbia
Protecting privacy. Promoting transparency.



Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner for British Columbia

PO Box 9038, Stn. Prov. Govt., Victoria, BC V8W 9A4
Telephone: 250.387.5629 | Toll Free in B.C.: 1.800.663.7867
E-mail: info@oipc.bc.ca | @BCInfoPrivacy

www.oipc.bc.ca